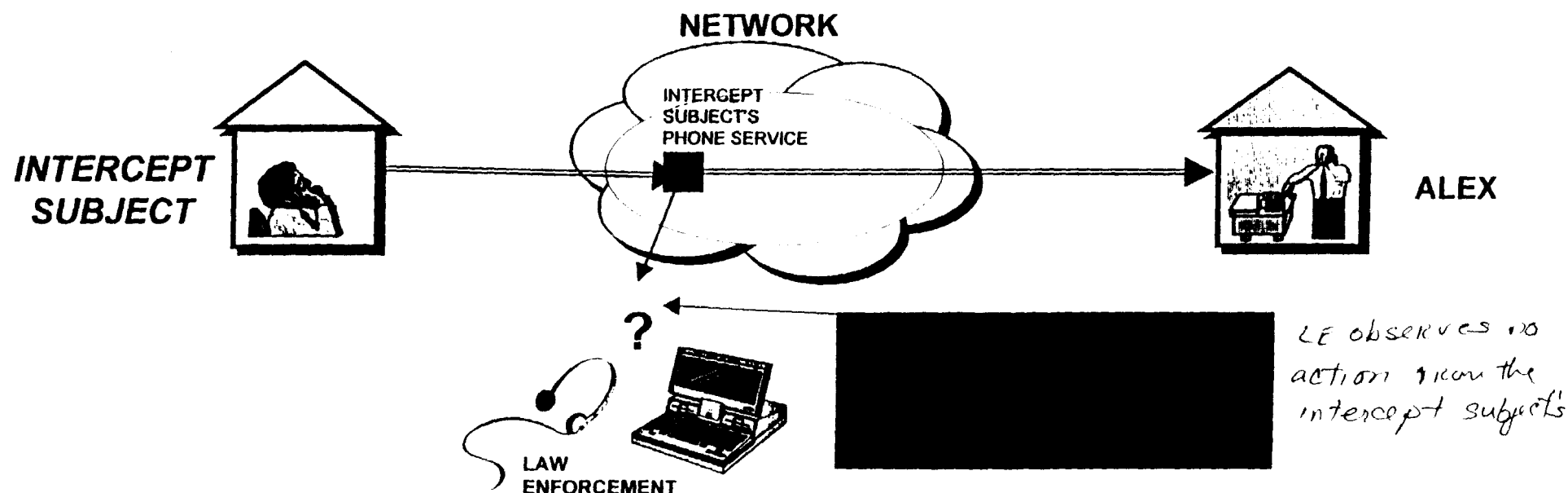


# Surveillance Status (Capabilities 6 and 7)

## Law Enforcement Needs To Know Status of Surveillance

- ③ Situation 2 (Circuit working but surveillance deactivated in the network)



LE calls the telephone carrier to check on the surveillance. Carrier notifies LE of the faulty connection, which caused LE to waste the manpower and miss several calls for those days. SP-3580A fails to provide the status of a surveillance. Law enforcement needs to be certain that the surveillance has not been deactivated in the network. Without this information, vital evidence could be lost if a surveillance is thought to be working when it is inactive.

# ***Missing Capabilities Eight***

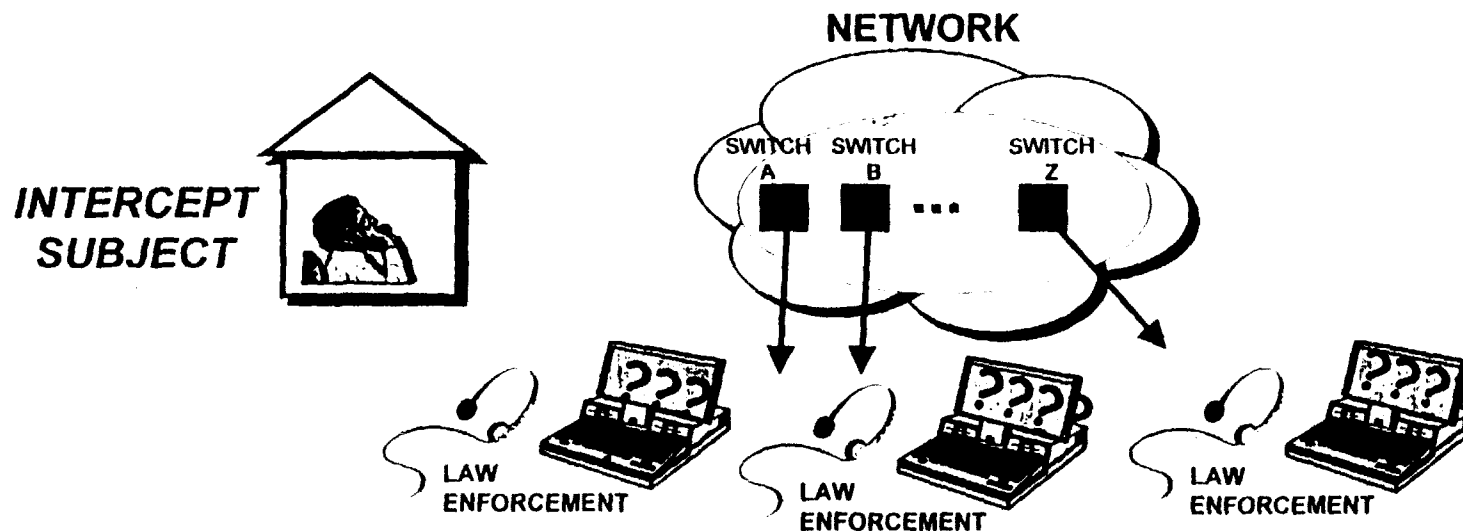
## ***Standard Delivery Interface***

***Law Enforcement Needs a Limited Number of Delivery Interfaces***

# ***Standard Delivery Interface (Capability 8)***

## ***Law Enforcement Needs a Limited Number of Delivery Interfaces***

---



Law enforcement has a court order to conduct electronic surveillance on the intercept subject's phone service. Law enforcement may not be able to interface with the switch serving the intercept subject. SP-3580A fails to limit the number of delivery interfaces. Law enforcement needs a limited number of delivery interfaces to be certain that the collection equipment will work with a specific carrier's network.

# ***Missing Capability Nine***

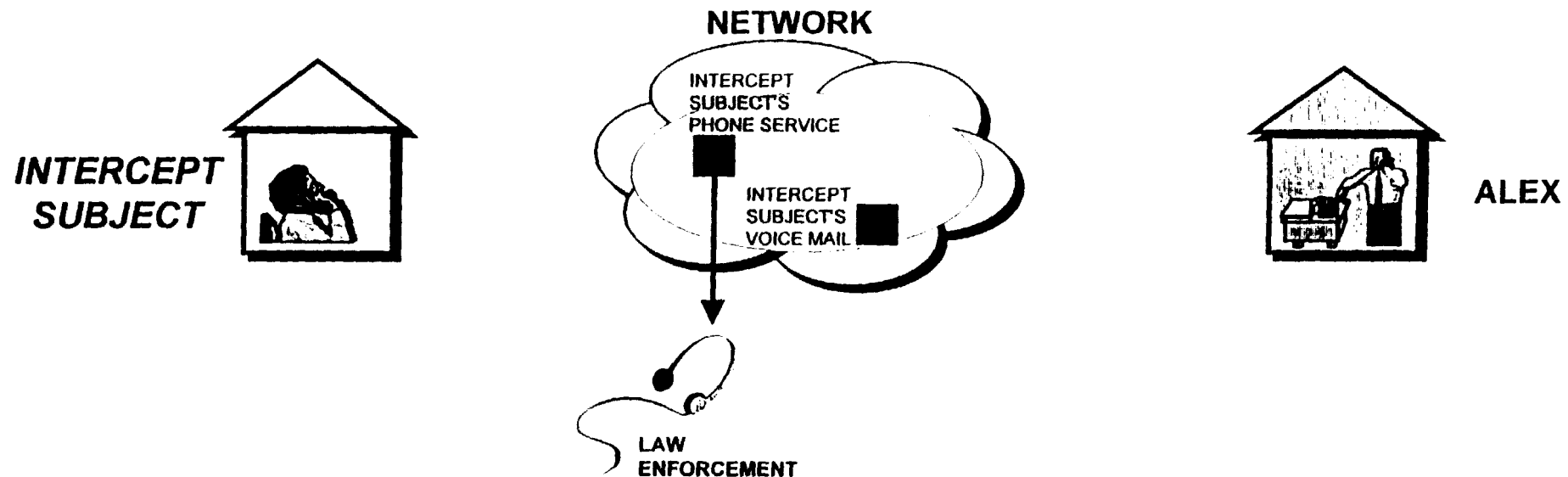
## ***Feature Status***

***Law Enforcement Needs Information on Changes to Feature Capabilities***

# Feature Status (Capability 9)

## Law Enforcement Needs Information on Changes to Feature Capabilities

①

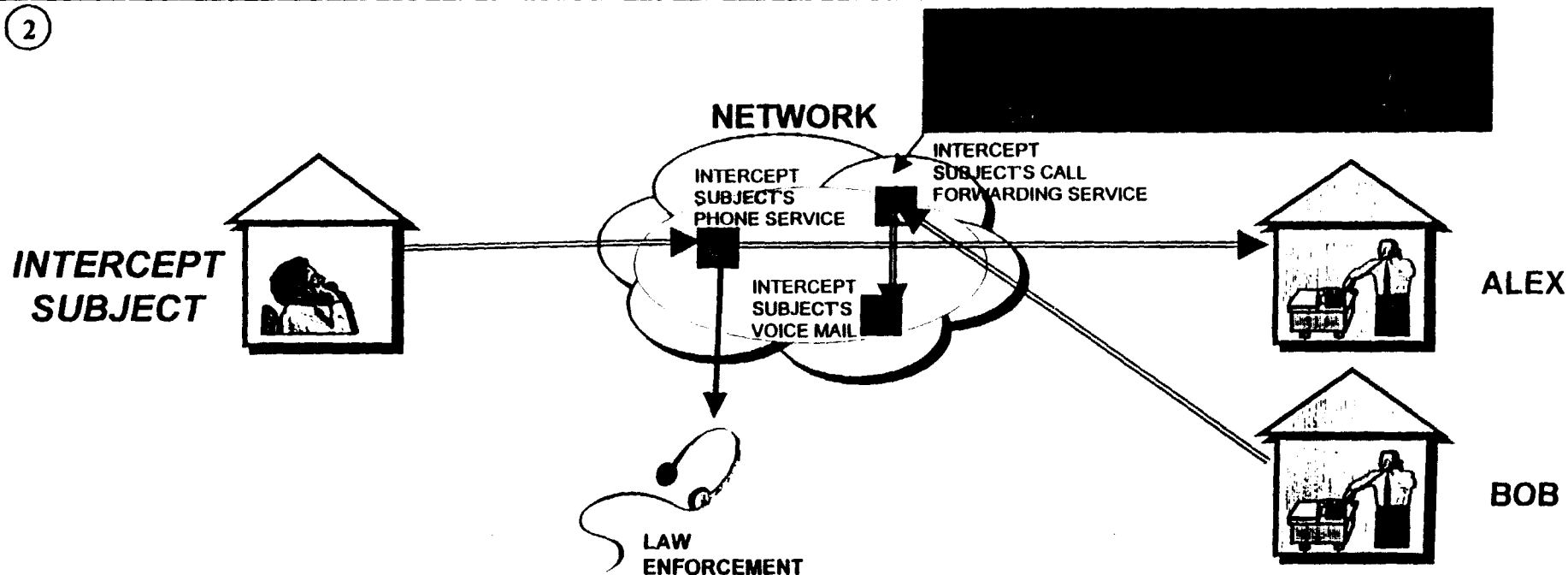


Law enforcement has a court order to conduct electronic surveillance on the intercept subject's phone service. Law enforcement has provisioned one circuit for the surveillance and is able to receive only one phone call at a time. Later, the intercept subject subscribes to Call Forwarding Busy to forward all calls to a voice mail system when he or she is on another call. Law enforcement is unaware of the change in the intercept subject's service. SP-3580A fails to provide notification that there has been a change in the intercept subject's feature capabilities.

# Feature Status (Capability 9)

## Law Enforcement Needs Information on Changes to Feature Capabilities

2



The intercept subject calls Alex. Later, Bob calls the intercept subject and is forwarded to the intercept subject's voice mail system. Law enforcement is unable to hear the message left for the intercept subject because only one surveillance circuit is available and it is in use. Law enforcement needs to know that the intercept subject has added features. With this information, additional surveillance circuits could be provisioned to monitor all possible calls placed to the intercept subject.

# ***Missing Capability Ten***

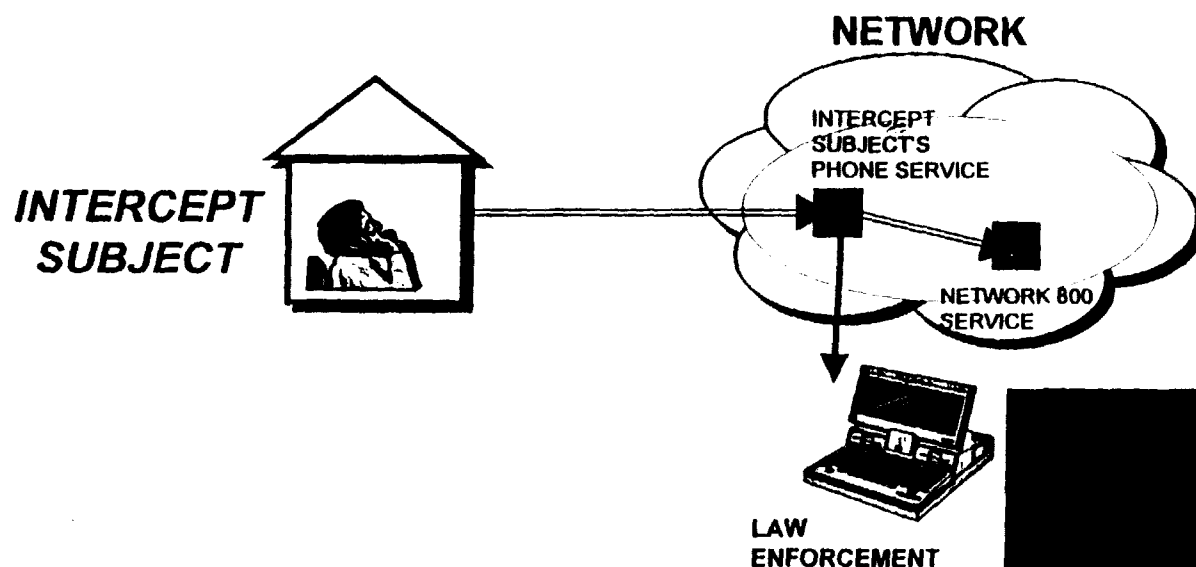
## ***Dialing Information***

***Law Enforcement Needs To Know Digits Dialed After Call is Connected***

# Dialing Information (Capability 10)

## Law Enforcement Needs To Know Digits Dialed After Call is Connected

①



LE receives the  
800 number only.  
The number entered  
during the call would  
not be sent to LE.

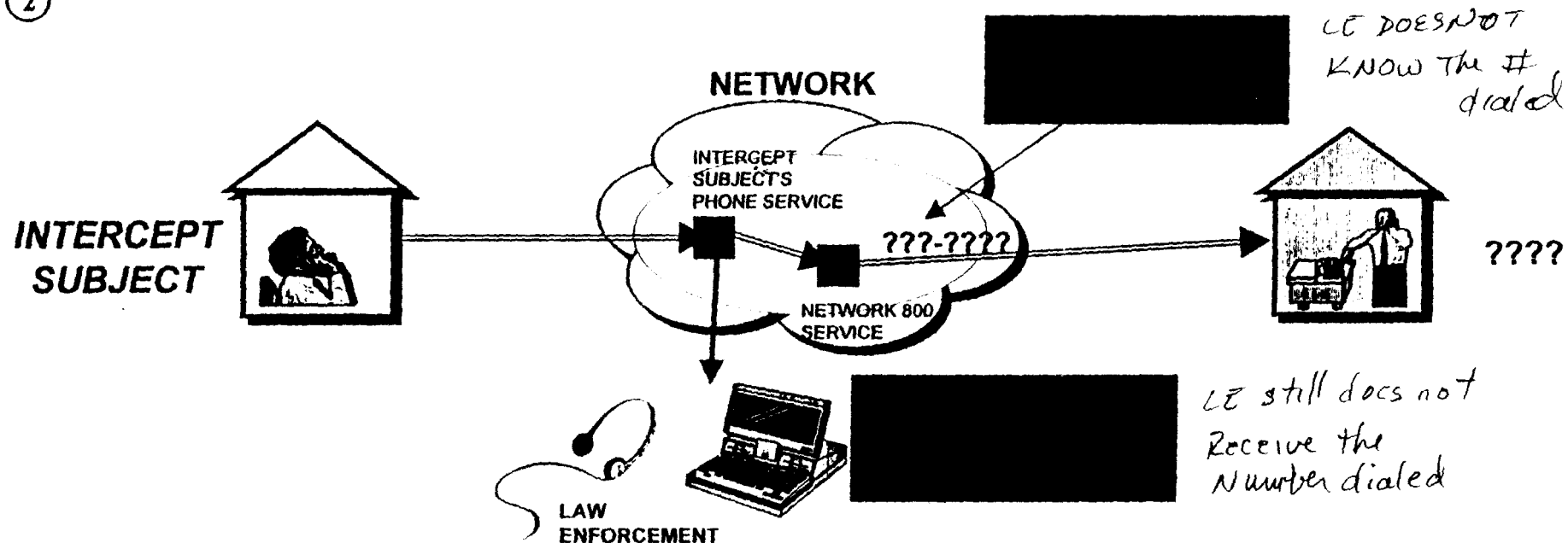
Law enforcement has a court order to conduct electronic surveillance on the intercept subject's phone service. The intercept subject dials 1-800-555-0000 to place a calling card call. A recorded announcement prompts the intercept subject to enter the number to call and a calling card number. The intercept subject enters the numbers. SP-3580A fails to provide the capability to receive the digits dialed after the call is connected.



# Dialing Information (Capability 10)

## Law Enforcement Needs To Know Digits Dialed After Call is Connected

2



The call is answered by the unknown party. Law enforcement needs to know the phone number associated with the party who answers the call so that the party can be identified. The intercept subject may have told this party information that could be used in court.

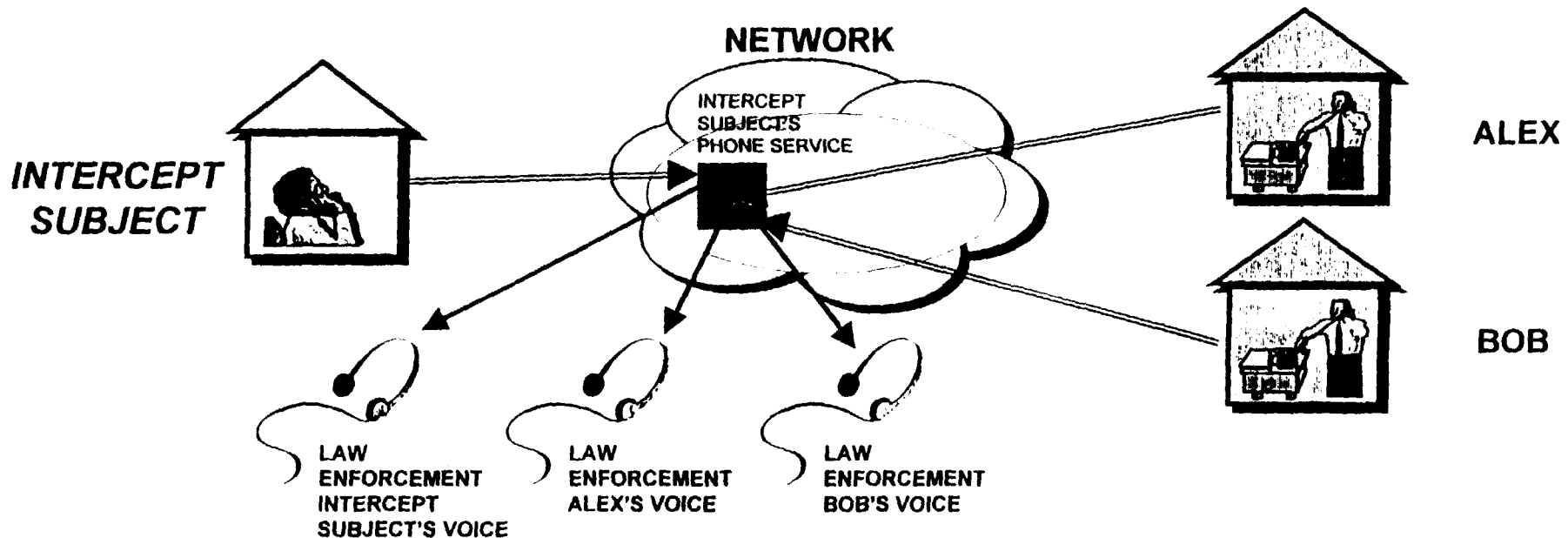
# ***Missing Capability Eleven***

## ***Separated Content***

***Law Enforcement Needs To Receive Each Party's Voice Separately***

# Separated Content (Capability 11)

**Law Enforcement Needs To Receive Each Party's Voice Separately**



Alex "flashes" to join everyone into a three-way conference call. SP-3580A fails to provide law enforcement with the capability to have each party's communications separated. Law enforcement needs the ability to receive the intercept subject, Alex, and Bob separately so that they can associate the conversations with the call identity information of each party. Without this association LE would not be able to associate communications of each party in the call. This capability's importance is further realized when more callers enter the conference call.



MEMORANDUM

December 5, 1997

To: Participants in December 3, 1997 Industry/FBI Engineering Summit

From: Grant Seiffert (202) 383-1483

Re: Overhead Summary of FBI Comments/Clarifications of the Punchlist

On December 3, 1997, engineers from telecommunications carriers and manufacturers and the Federal Bureau of Investigation conducted an engineering summit at TIA's offices in Arlington, Virginia. The purpose of the meeting was to discuss the twelve enhanced surveillance features requested by law enforcement ("the Punchlist").

The summit evolved from a November 12, 1997 meeting with Assistant Attorney General Steve Colgate. At the November meeting, Mike Warren, Section Chief for the CALEA Implementation Section (CIS) at the FBI, commented that he believed that industry was misinterpreting law enforcement's requests and that it might be possible to clarify these requests in such a way as to reduce the technical difficulty of providing the features.

During the summit, the FBI and other representatives of law enforcement responded to questions from industry manufacturers and elaborated upon the purpose for the twelve features. In general, law enforcement indicated that it is willing to compromise on what features each individual manufacturer provides and that it accepts that each manufacturer may not be able to provide every punchlist item.

In several instances (for example, timing, standard delivery interface, and feature status message), these discussions resulted in clarifications that appeared to reduce the technical difficulty of providing the feature. In at least one case (i.e., message of status surveillance), the clarification increased the perceived difficulty. The purpose of the summit was not to negotiate an industry/law enforcement agreement on each feature, simply to answer industry questions and clarify law enforcement's requests.

Overhead summaries of law enforcement's comments/clarifications were reviewed by all participants during the meeting for their accuracy. In addition, the clarifications were reviewed by the FBI for a second time yesterday. The final version of these overheads (with the FBI's subsequent comments underlined) is attached.

# facsimile TRANSMITTAL

---

**To:** Stewart Baker  
**Of:** Steptoe & Johnson  
**Fax:** 202-429-3902  
**Pages:** 4, including this cover sheet.  
**Date:** December 4, 1997

The following is the list of discussion points from yesterday's meeting. We have provided our comments which we've underlined. As mentioned in the meeting, the FBI is working in coordination with state and local law enforcement and will need their concurrence on each of these items.

From the desk of .

Dave Yarbrough  
Supervisory Special Agent  
Federal Bureau of Investigation  
14800 Conference Center Drive  
Chantilly, Virginia 20151  
703-814-4803  
Fax: 703-814-4720

**FBI Clarifications/Comments on "Punchlist" Features**  
(December 3, 1997)

**General Comments:**

This is a discussion paper produced during a meeting between law enforcement officials from the CALEA Implementation Section (CIS) and members of the Telecommunications Industry. It does not change government's requirements for the punch list. It does further clarify government's requirements and reflect flexibility for delivery of information. The law enforcement forum will need to review this paper. It is anticipated this review will occur December 18, 1997.

- Re: test suites -- Government will tailor what is compliant for each platform
- Willing to compromise on what the manufacturer provides; accepts that the punch list items may not be reasonably achievable by all manufacturers; manufacturer does not have to redesign its architecture

1. Timing (Capability 5)

- "Near real time" -- up to 10 seconds for 99% of calls (with in-band serial number on CCC linking call content to events); 3-5 seconds for 99% of calls (without serial number); 30 seconds unacceptable
- Manufacturer defines own demarcation point. Demarcation point is the point which separates network equipment and the government's transmission facilities
- More flexible for less important events; cross-reference to LE ballot comments which identify critical events

2. Standard Delivery Interface (Capability 8)

- Law enforcement does not expect a single interface; would prefer a limited set
- Willing to take what industry offers, but would prefer no more than 4 standard interfaces
- Willing to use manufacturers' preferred interface; interface will not necessarily be standardized but will be set through individual agreements between law enforcement and manufacturer-carrier pairings

3. Feature Status Message (Capability 9)

- Government does not require immediate notification; (e.g the 500 msec recommendation); willing to have this information on a regular basis once a day, not less than once every 24 hours) or [other solutions]
- Interested in a defined set of features that the feature status message would be used for (those that could hinder law enforcement's ability to conduct the intercept); exclude one-time features which all customers of a carrier receive simply by initiating service

#### 4. Network Signals (Capability 4)

- Not interested in all network signals; interested in a defined sub-set of user-perceived signals (each manufacturer is invited to provide its list of signals and law enforcement will identify the sub-set)
- Some user-perceived signals can be heard on the CCC and in those circumstances LE is willing to accept access to the CCC as opposed to separate signals on the CDC, but would prefer a separate message on the CDC

#### 5. Conference Calling: Who is Part of a Call at All Times (Capability 2)

- Only applies to reporting the switching connections made or broken by the switches supporting the subject's service; this does not apply to customer premises equipment (e.g., handset)

#### 6. Conference Calling: Conversations of Parties on Hold (Capability 1)

- Only covers conversations of two or more parties on hold
- If there is only one party on hold, there is no intercept requirement on that party
- This requirement covers not only parties "on hold" but also conversations continuing after the target hangs up, provided that the other parties continue to maintain their connection on that switch
- If the call is no longer maintained in the switch(es) serving the intercept subject, there is no requirement to continue the intercept
- 

#### 7. Dialing Information (Capability 10)

- Two ways to provide dialing information: (1) decipher and create messages for dialed digits, (2) provide CCC to law enforcement for deciphering
- If the solution involves DTMF, it is not necessary to provide a dedicated tone receiver for each intercept subject (at most, a receiver will be required for each simultaneous, in progress, intercept call)

#### 8. Feature Keys (Capability 3)

- Probably harder for wireline than wireless because, at this time, wireless has fewer feature keys
- LE only talking about physical keys which activate features for the intercept subject.



9. "Toggles"

- If a manufacturer's customers agree to accept all punchlist features, toggling capability will not be necessary
- Some features (timing, standard interface, etc.) cannot be toggled.
- LE willing to discuss with individual carriers and their manufacturers the possibility of grouping features to reduce cost of toggling
- In some cases, toggling will be difficult because it will require changes in hardware

10. Status of Surveillance: Message on Status of Surveillance (Capability 6)

- This is harder for wireless than wireline
- LE wants a message, which may be based on a poll, to determine that the interception is active on all nodes essential to the intercept
- This is more demanding than some manufacturers originally thought (because it requires checking so many distributed points)

11. Status of Surveillance: Continuity (tone) Check (Capability 7)

- LE interested in standard C-tone or some other signal indicating that connection is up

12. Separated Content (Capability 12)

- All parties recognize that this is the most difficult item on the list





U.S. Department of Justice

FEB - 3 1998

Washington, D.C. 20530

Mr. Tom Barba  
Steptoe & Johnson LLP  
Attorney at Law  
1330 Connecticut Avenue, NW  
Washington, DC 20036-1795

Dear Mr. Barba:

This letter confirms discussions held between the Department of Justice (DOJ), the Federal Bureau of Investigation (FBI), and representatives of the telecommunications industry during a January 23, 1998, meeting<sup>1</sup> regarding DOJ's position on the legal status under the Communications Assistance for Law Enforcement Act (CALEA) of the 11 electronic surveillance capabilities (referred to as the "punch list") that are missing from the current Telecommunications Industry Association (TIA) electronic surveillance standard J-STD-025. Additionally, it confirms the terms and conditions upon which DOJ will forbear bringing enforcement actions against industry members for non-compliance with CALEA.

**"Punch List"**

DOJ has reviewed the 11 "punch list" capabilities in reference to CALEA, its legislative history, and the underlying electronic surveillance statutes<sup>2</sup>. In addition, DOJ reviewed a memorandum evaluating the "punch list" under CALEA that was prepared by the Office of General Counsel (OGC) of the FBI. As a result of its

---

<sup>1</sup>Those in attendance at the January 23, 1998, meeting included representatives from the Cellular Telecommunications Industry Association (CTIA), Personal Communications Industry Association (PCIA), Telecommunications Industry Association (TIA), United States Telephone Association (USTA), Bell Atlantic, Department of Justice and the Federal Bureau of Investigation.

<sup>2</sup> CALEA was enacted to preserve the electronic surveillance capabilities of law enforcement commensurate with the legal authority found in the underlying electronic surveillance statutes, and so that electronic surveillance efforts could be conducted properly pursuant to these statutes.

review, DOJ is providing the following legal opinion: 9 of the 11 capabilities are clearly within the scope of CALEA and the underlying electronic surveillance statutes. These nine capabilities are<sup>3</sup>:

- Content of conferenced calls;
- Party Hold, Party Join, Party Drop;
- Access to subject-initiated dialing and signaling;
- Notification Message (in-band and out-of-band signaling);
- Timing to correlate call data and call content;
- Surveillance Status Message;
- Feature Status Message;
- Continuity Check; and
- Post cut-through dialing and signaling.

With respect to the first four capabilities (Content of conferenced calls; Party Hold, Party Join, Party Drop; Access to subject-initiated dialing and signaling; and Notification Message of in-band and out-of-band signaling), DOJ firmly believes that law enforcement's analysis and position regarding these assistance capability requirements satisfy CALEA section 103 requirements. These descriptions are set forth in the response submitted by the FBI<sup>4</sup> to TIA Committee TR45.2 during the balloting process on standards document SP-3580A.

With respect to the fifth through the ninth capabilities (Timing to correlate call data and call content; Surveillance Status Message; Feature Status Message; Continuity Check; and Post cut-through dialing and signaling), DOJ has also concluded that law enforcement's position satisfies CALEA section 103 requirements. Because of this opinion, discussion between the industry and law enforcement will be required in order to select a mutually acceptable means of delivering the information specified by each capability. Thus, if industry disagrees with law enforcement's proposed delivery method, it must affirmatively propose a meaningful and effective alternative.

Based upon the foregoing analysis, it is DOJ's opinion that TIA interim standard J-STD-025 is failing to include and properly address the nine capabilities listed above. Industry and law enforcement may wish to act in concert to revise the interim standard J-STD-025 to include solutions for each of these missing electronic surveillance capabilities.

---

<sup>3</sup> See Items 1-7, 9, and 10 of Attachment A.

<sup>4</sup> The FBI is closely coordinating its efforts with state and local law enforcement representatives across the nation. In this document "law enforcement" and "FBI" refer to this partnership and are used interchangeably.

With respect to capability number eight (Standardized Delivery Interface), although a single delivery interface is not mandated by CALEA, DOJ believes that a single, standard interface would be cost effective and of great benefit to both law enforcement and telecommunications carriers. Recent productive discussions with industry have resulted in what DOJ believes is an acceptable compromise, whereby the industry would commit to a limited number of no more than five delivery interfaces. DOJ supports such an agreement.

With respect to capability number 11 (Separated Delivery), DOJ, while recognizing the usefulness of such delivery for the effectiveness of electronic surveillance, nevertheless does not believe that CALEA section 103, or the underlying electronic surveillance statutes, require separated delivery.

Building on the progress made during the final months of 1997, the FBI's CALEA Implementation Section (CIS) will continue to work with solution providers<sup>5</sup> to reach an agreement on the technical feasibility of all the CALEA capability requirements.

#### **Forbearance**

During the January 23, 1998, meeting, the parties discussed the conditions under which DOJ would agree not to pursue enforcement actions against the carrier under section 108 of CALEA with regard to the CALEA mandate that a carrier meet the assistance capability requirements pursuant to CALEA section 103 by October 25, 1998, or against a manufacturer with respect to its obligation under CALEA section 106(b) to make features or modifications available on a "reasonably timely basis." A letter from the Office of the Attorney General, which was provided to all meeting attendees, outlined the basic conditions regarding forbearance:

In those situations where the carrier can foresee that it will not be able to meet the deadline because the manufacturer has yet to develop the solutions, the FBI is prepared to enter into an agreement with the manufacturer of the carrier's equipment wherein both parties (the FBI and a manufacturer) would agree upon the technological requirements and functionality for a specific switch platform (or other non-switch solution) and a reasonable and fair deployment schedule which would include verifiable milestones. In return, DOJ will not pursue an enforcement action against the manufacturer or carrier as long as the terms of the agreement are met in the time frames specified. DOJ

---

<sup>5</sup> Solutions providers include not only switch-based manufacturers, and support service providers, but other industry entities that are engaged in the development of network-based and other CALEA-compliant solutions.

will not pursue enforcement action against any carrier utilizing the switch platform (or non-switch solution) named in the agreement.

DOJ, in consultation with the FBI, has further elaborated on the conditions related to forbearance as follows:

Any member of the telecommunications industry seeking forbearance must submit to CIS a statement that identifies the following:

1. The CALEA capability requirements that will be included in its platform or designed into any non-switch-based solution.
2. The projected date by which the platform, or non-switch-based solution, will be made commercially available, the "commercially available date."
3. A timeline for design, development, and testing milestones that will be achieved by the manufacturer from the start of the project through the commercially available date, the "milestone timeline."
4. A schedule for furnishing information to CIS at each milestone to permit CIS to verify that a milestone has been reached.
5. A list of specific types of information to be provided according to the foregoing schedule.
6. A schedule for providing mutually agreed upon data to CIS from which the Government will be able to determine the fairness and reasonableness of the CALEA solution price.
7. A list of the specific types of price-related data to be provided.

With respect to item 1, the term "CALEA capability requirements" refers to the functions defined in the TIA interim standard J-STD-025 and the first nine punch list capabilities described earlier in this letter. Law enforcement will work with each solution provider as it produces a technical feasibility study to confirm its understanding of, and ability to meet, the CALEA capability requirements. For those switching platforms, or non-switch-based solutions, on which a capability is technically infeasible, law enforcement will consult with solution providers to assess the possibility of providing effective technical alternatives that will still provide law enforcement with the necessary evidentiary and minimization data sought by the capability.

With respect to item 2, the term "commercially available date" refers to the date when the platform or non-switch-based solution

will be made available by the solution provider for the immediate purchase and deployment by a carrier. That date shall, in no event, extend beyond the first currently scheduled software generic product release after the October 25, 1998, capability compliance date. With respect to item 3, the term "milestone timeline" refers to a schedule of the necessary design, development, and testing steps to be taken by a solution provider in making a product commercially available. With respect to item 4, a solution provider is expected to include a schedule specifying the time after the completion of each milestone when CIS will be able to verify that the milestone has been reached. With respect to item 5, the specific types of information contained in the affirmative confirmation of the foregoing schedule will include, but not be limited to, draft design documents, feature specification documents, and test results. With respect to item 6, a solution provider is expected to provide a schedule detailing the delivery to CIS of all necessary information for the government to make a determination of the fairness and reasonableness of the price of the solution provider's commercially available CALEA solution. With respect to item 7, the specific types of information contained in the price-related information of the foregoing schedule will include, but not be limited to, market prices of comparable features with similar levels of design, development, and testing effort.

Forbearance for a solution provider, and its carrier customers, will be conditioned upon its ability to provide the above listed items as well as to meet verifiable solution development milestones. A solution provider's failure to meet these milestones will result in the loss of forbearance for the solution provider.

Carrier forbearance ends with the commercial availability of a solution. Switches, or portions of a network, of historical importance to law enforcement for which the government must reimburse the carrier will be identified by CIS. Equipment, facilities, and services installed or deployed after January 1, 1995, will be included in any forbearance until a solution is commercially available. Following solution availability, for those switches or portions of a network not identified by CIS, carriers are expected to follow their normal deployment processes in determining which switches, or portions of their networks, will be upgraded with the CALEA capabilities. Figure 1 illustrates the basic elements of forbearance.

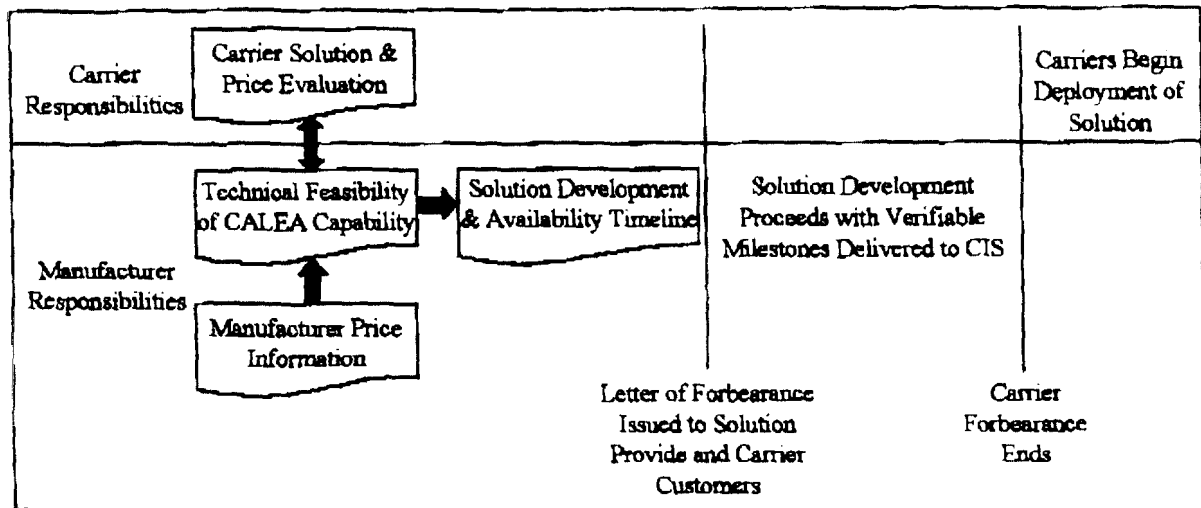


Figure 1: Forbearance

The foregoing forbearance discussion centers on two separate and distinct agreements: Agreements in Principle (AIP) between the FBI and a solution provider, and Cooperative Agreements between the FBI and a carrier.

In an AIP, the FBI and solution providers agree that solution providers have complied with the seven criteria listed above, including a feasibility analysis and pricing information for CALEA capability requirements. The feasibility analysis and pricing information will allow the government to finalize its position regarding the standard, extension of the compliance dates, forbearance, etc. The FBI, in consultation with law enforcement, will not be in a position to make critical determinations until the information described in the above seven criteria has been provided.

Currently many versions of draft AIPs are circulating, both FBI- and industry-generated, and some are more comprehensive than is presently warranted. Some of the AIPs in circulation were derived from an AIP drafted by TIA. The FBI hopes to meet with TIA during the week of February 2, 1998, to discuss the proposed AIP. The results of these discussions will then be disseminated to TIA's membership and any other interested solution provider.

The Cooperative Agreement, on the other hand, is the contractual vehicle whereby telecommunications carriers will receive reimbursement for their eligible CALEA costs. Cooperative Agreements may be executed for different purposes at different stages of CALEA implementation. For example, an initial round of Cooperative Agreement negotiations is taking place to establish contractual vehicles whereby carriers selected to support specific solution providers with the feasibility analyses and pricing information may receive reimbursement for assisting in




this effort. Unfortunately, this initial round of negotiations has encountered some problems. One of the issues is the clarification of a carrier's role in assisting in the analysis of the solution provider's proposed solution. It appears from discussions with carriers that a mutual understanding of the intent of the government's proposed language for the Cooperative Agreements and its Statement of Work (SOW) does not yet exist. Carriers commented that the SOW included a consultative role that the carriers are unable or unwilling to perform. Although it was the government's intent to construct an SOW flexible enough to allow carriers to accommodate their normal roles in the solution provider product development process, the proposals received in response to the SOW have been too non-specific to provide real value.

The FBI still believes, and has had it confirmed by solution providers, that carriers have an essential role to play in developing the CALEA solution. The FBI will now request that each solution provider describe in detail the typical interaction it might have with one of its carrier customers during new product development. These descriptions will then be incorporated into the proposed SOWs, which the government will seek from carriers.

Your continued willingness to work with law enforcement toward the development of electronic surveillance solutions is greatly appreciated.

Sincerely,

  
 Stephen R. Colgate  
 Assistant Attorney General  
 for Administration